実施：2025 年 1 月 20 日 (月) 9:10-10:40, E-601 室

2024 年度　**後 期　定 期 試 験** (問題 兼 解答用紙)

開講学部	評点小計
理工学部	

評　点
/120

(集計後に 100 点満点に換算)

問題枚数	両面印刷	別紙解答用紙	試験時間	試 験 科 目 名	クラス	出 題 者
2	有	なし	80 分	代 数 学 5　月曜 1 時限, 教科書：Original　(§§1 − 11)	A, B	大 西 良 博

持込許可物件	所属学部	所属学科	学年	学 籍 番 号 (9 桁)	氏　名
なし	理工学部	数学科	年		

注意 1. 最終的な答に至る途中の説明をできるだけ詳しく書くこと．最終結果だけでは得点できない．

注意 2. 試験場の静粛を保つために，退出は開始 60 分後の時点の一回限りとする．

注意 3. 学生証，記名用のペン，鉛筆またはシャープペンシル，消しゴム以外は机の上に置かないこと．

注意 4. $\boxed{\mathbf{8}}$ は選択問題である．$\boxed{\mathbf{8a}}$ $\boxed{\mathbf{8b}}$ のどちらかを選んで解答せよ．

注意 5. i は虚数単位を表し，$\omega = \frac{-1+\sqrt{3}\,i}{2}$ である．これらの記号は自由に使ってよい．

$\boxed{\mathbf{1}}$ (10 点)　K は標数 $p>0$ の体とする．任意の元 $a, b \in K$ に対し，次の問に答へよ．

(1) 一般に自然数 $m \geqq 2$ と $1 \leqq r \leqq m-1$ なる自然数 r について，2 項係数 $\binom{r}{m}(= {}_m\mathrm{C}_r)$ は m で割り切れるとは限らないことを具体例で示せ．

(2) $1 \leqq r \leqq p-1$ のとき，2 項係数 $\binom{r}{p}$ は p で割り切れることを示せ．

(3) $(a+b)^p = a^p + b^p$ が成り立つことを示せ．

(4) 任意の $n \in \mathbb{N} \cup \{0\}$ について　$(a+b)^{p^n} = a^{p^n} + b^{p^n}$ が成り立つことを示せ．

$\boxed{\mathbf{2}}$ (10 点)　$f(x) = x^3 + x^2 + x + 3$ は $\mathbb{F}_5[x]$ の既約多項式である．これの根の 1 つを α とし $K = \mathbb{F}_5(\alpha)$ とせよ．このとき，K において

$$\frac{1}{\alpha^2 + 4\alpha + 1}$$

を α の $\mathbb{F}_5$ 上の 2 次以下の多項式で表せ．

$\boxed{\mathbf{3}}$ (10 点)　次の体の間の包含関係を Hasse 図で示せ：

$\mathbb{Q}$,　$\mathbb{Q}(\sqrt{2})$,　$\mathbb{Q}(\sqrt{2i})$,　$\mathbb{Q}(\sqrt[4]{2})$,　$\mathbb{Q}(\sqrt[4]{2}\,i)$,　$\mathbb{Q}(\sqrt[6]{2}\,i)$,　$\mathbb{Q}(i)$.

但し，$\sqrt{}$ の "屋根" の長さに注意せよ．さらに，隣接する体の間の <u>拡大次数</u> も書き入れよ．理由の説明も可能な限り記入せよ．

学 籍 番 号 (9 桁)	氏　　名

4 (10 点) 代数的拡大 L/K に対し, $L \supset R \supset K$ なる環 R は体であることを示せ. 但し, R の演算は L で定義されてゐる演算によるものとする.

5 (10 点) 体の拡大 L/K と $\alpha, \beta \in L$ について,

$$[\,K(\alpha):K\,] = m,\ \ [\,K(\beta):K\,] = n,\ \ \gcd(m,n) = 1$$

とせよ. このとき

$$[\,K(\alpha,\beta):K\,] = mn$$

であることを示せ.

6 (10 点) 次の体の合成体のできるだけ簡潔な表記とその $\mathbb{Q}$ 上の基底, および $\mathbb{Q}$ 上の拡大次数を求めよ.

(1) $\mathbb{Q}(\sqrt[4]{2}\,)$ と $\mathbb{Q}(\sqrt[3]{4}\,)$　　　(2) $\mathbb{Q}(\omega)$ と $\mathbb{Q}(\sqrt{5}\omega\,)$

7 (10 点) 代数的拡大 L/K とそれの互ひに包含関係がない 2 つの真の部分体 M_1, M_2 で次の様な例を挙げよ. 説明も付けること.

(1) $[\,M_1M_2 : M_1\,] < [\,M_2 : K\,]$ かつ $[\,M_1M_2 : M_1\,] = [\,M_2 : M_1 \cap M_2\,]$

(2) $[\,M_1M_2 : M_1\,] < [\,M_2 : M_1 \cap M_2\,]$.

学 籍 番 号 (9 桁)	氏 名

8a (10 点) 体の同型について, 以下の問に答へよ.
(1) 体 $\mathbb{Q}(\sqrt[4]{3})$ の自己同型をすべて求めよ.
(2) 体 $\mathbb{Q}(\sqrt[4]{3})$ から $\mathbb{C}$ への中への同型をすべて求めよ.

8b (10 点) p を素数とし, t を不定元とする. $\varphi : \mathbb{F}_p(t) \longrightarrow \mathbb{F}_p(t)$, $\varphi(\alpha) = \alpha^p$ は中への同型であることを示せ. また, この写像の像の体を記せ.

9 (10 点) 体の拡大 L/K があり, $\alpha, \beta \in L$ は K 上代数的とせよ.
$\mathrm{irr}\,(\alpha, K, x) = \mathrm{irr}\,(\alpha, K(\beta), x) \iff \mathrm{irr}\,(\beta, K, x) = \mathrm{irr}\,(\beta, K(\alpha), x)$
を示せ.

10 (10 点) 次の多項式 $f(x) \in \mathbb{Q}[x]$ について, $f(x)$ の最小分解体とその $\mathbb{Q}$ 上の拡大次数を求めよ. 最小分解体はできるだけ簡潔な表示を求む.
(1) $f(x) = x^4 - x^2 - 12$ (2) $f(x) = (x^2+1)(x^2+2x+2)$ (3) $f(x) = x^4 + 5x^2 + 9$.

学 籍 番 号 (9 桁)	氏　　名

$\boxed{\textbf{11}}$ (10 点) 次の拡大は正規拡大であるか否か.
それぞれ理由を付けて答へよ.

(1) $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$　　(2) $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$　　(3) $\mathbb{Q}(\sqrt{2i}, \sqrt[4]{3})/\mathbb{Q}$

$\boxed{\textbf{12}}$ (10 点) t を不定元とする. 次の拡大は正規拡大であるか否か.
それぞれ理由を付けて答へよ. (Hint : $\mathbb{F}_7{}^\times = \langle 3 \rangle$)

(1) $\mathbb{F}_7(t)/\mathbb{F}_7(t^7)$　　(2) $\mathbb{F}_7(t)/\mathbb{F}_7(t^6)$　　(3) $\mathbb{F}_7(t)/\mathbb{F}_7(t^3)$

記　号

$\mathbb{N}$ … 自然数全体, $\mathbb{Z}$ … 整数全体のなす環, $\mathbb{Q}$ … 有理数全体のなす体,
$\mathbb{R}$ … 実数全体のなす体, $\mathbb{C}$ … 複素数全体のなす体.　$\omega = \frac{-1+\sqrt{3}i}{2}$.

既習事項のまとめ

(1) 体 L の部分集合 K が L の演算に関して体であるとき, K を L の部分体, あるいは L は K の拡大といひ, この状況を体の拡大 L/K と記す.

(2) 体の拡大 L/K に対して K 上の vector 空間としての L の次元を L/K の拡大次数と呼び $[L:K]$ で表す. 3 つの体 $K \subset M \subset L$ について $[L:K]=[L:M][M:K]$.

(3) 体の拡大 L/K について, 任意の $\alpha \in L$ がある $f(x) \in K[x]$ の根であるとき, L/K を代数的拡大と呼ぶ.

(4) 体の拡大 L/K について, $[L:K]<\infty$ のとき, これを有限次拡大と呼ぶ.

(5) 体 K が体 M の部分体で, M が体 L の部分体であるとき, M を L/K の中間体と呼ぶ.

(6) 体 L とその部分体 K および $\alpha_1, \cdots, \alpha_n \in L$ に対し, K のすべての元と $\alpha_1, \cdots, \alpha_n$ をすべてを含む最小の体を $K(\alpha_1, \cdots, \alpha_n)$ と記す. これは K に係数をもつ様な $\alpha_1, \cdots, \alpha_n$ の有理式の全体に他ならない.

(7) ある体 L がその部分体 K と $\alpha \in L$ によつて, 上の記法で $L=K(\alpha)$ と書けるとき, L は K の単純拡大であるといはれる.

(8) 2 つの部分体の共通部分は再び体であるから, どんな体 K についても, それに含まれる最小の体が存在する. それを素体と呼ぶ. 素体は有理数体 $\mathbb{Q}$ か p 元体 $\mathbb{F}_p=\mathbb{Z}/p\mathbb{Z}$ (p は素数) に同型である.

(9) 体 K の積に関する単位元 1 をいくつか加へて 0 になるとき, その最小の個数は K の標数といはれ, それは素数である. 1 をいくつ加へても 0 にならない場合は, 標数は 0 であるといふ. K 標数を $\mathrm{char}\,K$ と記す. 前者の場合は素体が $\mathbb{F}_p$ であり, 後者の場合の素体は $\mathbb{Q}$ である.

(10) 拡大 L/K と $\alpha \in L$ について, α を根とし, 最高次係数が 1 であり, 次数が最小な多項式 $f(x)=K[x]$ が唯 1 つ存在し, それを α の最小多項式と呼んで $\mathrm{irr}(\alpha, K, x)$ で表す.

(11) 拡大 L/K と中間体 M_1, M_2 について, M_1 と M_2 を含む最小の部分体を M_1M_2 または M_2M_1 と書いて, M_1 と M_2 の合成体と呼ぶ. また, 拡大 M_1M_2/M_1 を拡大 M_2/K の M_1 による持ち上げと呼ぶ.

(12) 体 K を含む体 Ω 上に代数的拡大が存在しないとき, Ω は代数的閉体といはれ, さらにもし, Ω/K が代数的拡大であるならば Ω は K の代数的閉包といはれる. 任意の体 K に対し, その代数的閉包が存在し, すべて同型である. それを一般に $\overline{K}$ と記す.

(13) 多項式 $f(x) \in K[x]$ のすべての根で K 上される様な体を $f(x)$ の最小分解体といふ.

(14) 拡大 L/K が, どんな既約多項式 $f(x) \in K[x]$ も L 内に 1 つ根を持てば, $f(x)$ が L 上 1 次式のみの積に分解する, といふ性質を持つとき, L/K は正規拡大であるといはれる.

(15) 正規拡大の“底上げ”($L \supset M \supset K$ についての L/K の主張を L/M に乗り換へること) や持ち上げは正規拡大である. また K 上の 2 つの正規拡大の合成体はまた K 上の正規拡大である.

以上が「代数学 5」の範囲.

(16) 多項式 $f(x) \in K[x]$ が重根を持たないとき, $f(x)$ は分離的であるといはれる. 拡大 L/K において, $\alpha \in L$ が K 上の分離的多項式の根であるとき α は K 上分離的であるといはれ, さらに, すべての $\alpha \in L$ が K 上分離的であるとき, L/K を分離的拡大と称する.

(17) 分離的拡大の持ち上げは分離的拡大である. また K 上の 2 つの分離的拡大の合成体はまた K 上の分離的拡大である.

(18) あらゆる代数的拡大 L/K が分離的である様な体 K は完全体と呼ばれる. 標数が 0 である体や有限体は完全体である.

(19) 代数的拡大 L/K について, L から $\overline{K}(\supset L)$ への中への K 上の同型の個数を $[L:K]_s$ と記す. さらに $[L:K]_i=[L:K]/[L:K]_s$ と記す. $\mathrm{char}\,K=p>0$ のとき, これは p の冪になる.

(20) 分離的拡大は単純拡大である.

(21) 正規かつ分離的な代数的拡大を Galois 拡大と呼ぶ.

(22) 有限次 Galois 拡大 L/K とその Galois 群 $G=\mathrm{Gal}(L/K)$ について, $\mathscr{F}(L/K)$ を L/K の中間体の全体, $\mathscr{G}(G)$ を G の部分群の全体とせよ. 各 $H \in \mathscr{G}(G)$ に対し $L^H=\{\alpha \in L \,|\, \alpha^\sigma=\alpha\ (\forall \sigma \in H)\}$, 各 $M \in \mathscr{F}(L/K)$ に対し $G^M=\{\sigma \in G \,|\, \alpha^\sigma=\alpha\,(\forall \alpha \in M)\}$ と記す. このとき $G^M=\mathrm{Gal}(L/M)$ である.

(23) Galois の基本定理 1
(22) の状況下で, $\varphi: H \mapsto L^H$ は $\mathscr{G}(G)$ から $\mathscr{F}(L/K)$ への包含関係を逆転させる全単射であり, 逆写像は $\varphi^{-1}(M)=G^M$ で与へられる.

(24) Galois の基本定理 2
(22) の状況下で, $M \in \mathscr{F}(L/K)$ について次が成り立つ.
(1) $\tau \in \mathrm{Gal}(L/K)$ に対し, $\tau\,\mathrm{Gal}(L/M)\tau^{-1}=\mathrm{Gal}(L/M^\tau)$.
(2) M は K の Galois 拡大 $\iff$ $\mathrm{Gal}(L/M) \lhd \mathrm{Gal}(L/K)$.
(3) (2) の両側が成り立つとき, $\mathrm{Gal}(M/K) \simeq \mathrm{Gal}(L/K)/\mathrm{Gal}(L/M)$ (群としての同型).

(25) Galois 群が巡回群である様な拡大は, 巡回拡大と呼ばれる.

(26) Galois 群が Abel 群である様な拡大は, Abel 拡大と呼ばれる.

(27) 体 K 上の Abel 拡大の合成体は K 上の Abel 拡大である.

(28) 拡大 L/K の部分体 M, M' について M/K と M'/K がともに Galois 拡大であれば, MM'/K も Galois 拡大であつて, $\mathrm{Gal}(MM'/K) \simeq \mathrm{Gal}(M/M \cap M')$ が成り立つ. 左辺の σ に対して右辺の $\sigma|_M$ が対応する.